Text of Regulations

California Code of Regulations
Title 11. Law
Division 1. Attorney General
Chapter 18. Electronic Recording Delivery System
Article 5. Baseline Requirements and Technology Standards

§ 999.129. Standards and Guidelines.

Standards and guidelines contained in these regulations are based on NIST and FIPS publications including: NIST Special Publication 800-88, Guidelines for Media Sanitization (publication date September 2006); FIPS 180-~~2~~3, Secure Hash Standard (publication date ~~August 2002~~October 2008 ~~with change notice dated February 2004~~); FIPS 140-2, Security Requirements for Cryptographic Modules (publication date May 2001 with a change notice dated December 2002); FIPS 197, Advanced Encryption Standard (publication date November 2001); FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC) (publication date ~~March 2002~~July 2008); NIST Special Publication 800-63-1, Electronic Authentication Guideline (publication date ~~April 2006~~December 2011 ~~Version 1.0.2~~); NIST Special Publication 800-70, ~~Security Configuration Checklists Program for IT Products~~National Checklist Program for IT Products-Guideline for Checklist Users and Developers (publication date ~~May 2005~~February 2011). The ERDS Program shall make available any update, revision or replacement of a reference cited.

Note: Authority cited: Section 27393, Government Code. Reference: Section 27393(b), Government Code.

§ 999.133. Payload Structure, Content and Usage.

…

(e) Multiple digital electronic records or digitized electronic records within the same payload are ~~is~~ allowed; Only Secure Access users are authorized to include both Type 1 and Type 2 instruments in the same ERDS payload. ~~however, Type 1 and Type 2 instruments may not be included in the same ERDS payload.~~

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27391(e), 27392(b) and 27393(b)(10), Government Code.

§ 999.137. Security Requirements for Payload Protection.

(a) All ERDS for either Type 1 or Type 2 instruments shall employ encryption, both in transmission and storage, until decrypted by the intended recipient to protect the confidentiality of ERDS payloads using the encryption algorithms specified in the latest final NIST/FIPS publication. Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program. ~~Once decrypted by the intended recipient, the security of the~~

~~contents shall become the responsibility of the intended recipient. Two payload encryption algorithms are approved for ERDS:~~

~~(1) The RSA Algorithm using a minimum key-length of 1024 bits; and~~

~~(2) The Advanced Encryption Algorithm using a minimum key-length of 128 bits as defined in FIPS 197, Advanced Encryption Standard (publication date November 2001).~~

(b) All ERDS for either Type 1 or Type 2 instruments shall use hashing to protect the integrity of ERDS payloads utilizing the hash algorithm specified in the latest final NIST/FIPS publication. Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program. ~~The hash function approved for ERDS payloads is the Secure Hash Algorithm defined in FIPS 180-2, Secure Hash Standard (publication date August 2002 with change notice dated February 2004), using a message digest size of at least 224 bits.~~

(c) All ERDS for either Type 1 or Type 2 instruments shall use Digital Signatures to assure the authenticity of ERDS payloads utilizing the latest final Digital Signature Standard NIST/FIPS publication. Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program.~~The signing function approved for ERDS payloads is the RSA algorithm, using a minimum key-length of 1024 bits.~~

(d) All ERDS for either Type 1 or Type 2 instruments shall use a Public Key Infrastructure (PKI) established by the County Recorder to ensure all ERDS users are uniquely identified and to protect the integrity and authenticity of ERDS payloads. The public/private key-pair shall constitute the user's PKI identity credentials. Cryptographic modules used for generating encryption keys shall meet the requirements of the latest final NIST/FIPS publication. Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program~~Security Level 2 defined in FIPS 140-2, Security Requirements for Cryptographic Modules (publication date May 2001 with a change notice dated December 2002)~~.

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b) and 27397.5, Government Code.

§ 999.139. Security Requirements for Computer Media.

…

(b) Fixed and removable disks for either Type 1 or Type 2 instruments shall be sanitized as defined in the latest final NIST Special Publication, ~~800-88, Guidelines for Media~~

~~Sanitization (publication date September 2006),~~ prior to reallocating ERDS hardware or storage media to other purposes.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.141. ERDS Authentication Security Requirements.

(a) ERDS that serve Type 1 and 2 instruments shall be required to meet all of the additional authentication security requirements required for Type 1 instruments as follows:

…

(2) Authentication assurance shall meet Level 3 or higher, as defined by the latest final NIST Special Publication ~~800-63,~~ for Electronic Authentication Guideline. ~~(publication date April 2006 Version 1.0.2).~~ Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program.

(3) The token methods described by the NIST may be used, provided that authentication assurance Level 3 or higher, as defined by the latest final NIST Special Publication ~~800-63,~~ for Electronic Authentication Guideline. ~~(publication date April 2006 Version 1.0.2), is achieved.~~ Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program.

…

Note: Authority cited: Section 27393(b), Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.143. ERDS Server Security Requirements.

(a) ERDS that employ one or more servers that serve Type 1 or Type 1 and 2 instruments shall be required to meet all of the additional server security requirements for Type 1 instruments as follows:

…

(8) At a minimum, servers shall be hardened according to the standards established by the latest final NIST/FIPS publications or the manufacturers recommended guidelines. ~~the County Recorder.~~ The County Recorder shall ensure that all county servers used for ERDS are "hardened" according to such standards. Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication or latest manufactures recommended guidelines to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program. ~~one of the following checklists or guidelines:~~

~~(A) NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products (publication date May 2005).~~

(A~~B~~) Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.144. ERDS Security Requirements for Network Security.

(a) ERDS that serve Type 1 or Type 1 and 2 instruments shall be required to meet all of the additional network security requirements for Type 1 instruments as follows:

…

(3) The standard for establishing secure connection is ~~the TLS protocol as~~ described in the latest final NIST Special Publication ~~800-63,~~ for Electronic Authentication (~~publication date April 2006 Version 1.0.2).~~Currently, TLS protocol as of April 2011). As a minimum, 128-bit encryption shall be utilized. To establish secure transport layer security sessions, as described in the latest final FIPS publication for encyption (Currently Advanced Encryption Standard as of April 2011). Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any extensions require written justification for review by the ERDS Program.~~used to establish secure TLS sessions, as described in FIPS 197, "Advanced Encryption Standard", (publication date, November 2001).~~

(4) ERDS shall employ MAC to assure the ~~authenticity~~ authentication of encrypted ERDS payloads. ~~Each~~ MACs shall conform to the latest final FIPS standard regarding ~~defined in FIPS 198, "The~~ Keyed-Hash Message Authentication Code (HMAC)."~~;~~ Certified ERDS has a period of up to 6 months from the date of the latest final NIST/FIPS publication to update their systems for compliance. Such an update is to be considered a substantive modification. Any exentsions require written justification for review by the ERDS Program. ~~(publication date March 2002).~~

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2) and 27397.5, Government Code.

§ 999.145. Physical Security.

…

(b) All ERDS that serve either Type 1 or Type 2 instruments shall be required to meet all of the physical security requirements as follows:

(3) During local inspections, ERDS Program ~~staff~~representative shall be allowed to inspect all access requests and inventory reports that occurred within the 2-year period prior to the start of a local inspection.

…

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27393(b)(2), 27393(c) and 27397.5, Government Code.

§ 999.146. Auditable Events, Incidents and Reporting.

…

(d) All of the following are auditable ERDS events for both Type 1 or Type 2 instruments, unless otherwise stated, that shall be logged, and, when applicable, processed only as an incident or processed as an incident and reported.

…

(7) For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas~~; or any user attempting to use ERDS software and/or interfaces in a non-ERDS manner~~. This is an incident and shall be reported if fraud is suspected.

(8) Use of expired or revoked credentials. This is an incident and shall be reported if fraud is suspected.

(9) For Type 1 only, privilege elevation. This is an incident and shall be reported.

(10) For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session. This is an incident and shall be reported if fraud is suspected.

~~(11) For Type 1 only, unauthorized user gaining access to an ERDS server or ERDS payload storage area by using ERDS credentials. This is an incident and shall be reported.~~

~~(12) Any user gaining access using expired or revoked credentials. This is an incident and shall be reported.~~

(11~~3~~) Authentication failures.

(12~~4~~) ERDS accounts locked out and/or disabled due to failed consecutive login attempts. This is an incident and shall be reported if intrusion is suspected.

(13~~5~~) Auditable events overwrite other logged events. This is an incident and shall be reported if intrusion is suspected.

(14~~6~~) Auditable events cannot be logged. This is an incident.

(15~~7~~) Logs consume 95% or more of the storage space allocated for logging. This is an incident.

(168) Logs cannot be safely stored. This is an incident.

(179) For Type 1 only, ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not. This is an incident only if not authorized and shall be reported if fraud is suspected.

(1820) For Type 1 only, hardware or software configuration changes. This is an incident only if not authorized and shall be reported.

(1921) Unique name of the ERDS payload. This is an incident only if out of sequence.

(202) Dates and times the ERDS payload was submitted, retrieved or, when applicable, returned. This is an incident only if the dates and times are not current.

(213) Identity of the individual, who submitted, retrieved or, when applicable, returned the ERDS payload. This is an incident only if not authorized;.

(224) Name of the organization that the individual represented while submitting, retrieving or, when applicable, returning the ERDS payload**.** This is an incident only if not authorized.

(235) For Type 1 only, a transmission failure.

(246) For Type 1 only, a storage failure.

(257) A decryption failure. This is an incident and shall be reported if fraud is suspected.

(268) A hash failure. This is an incident and shall be reported if fraud is suspected.

(279) A validity check failure. This is an incident and shall be reported if fraud is suspected.

(2830) Type 1 or Type 2 instrument submitted unencrypted. This is an incident and shall be reported.

(2931) Type 1 instrument submitted as a Type 2 instrument or vice versa. This is an incident and shall be reported if fraud is suspected.

(302) Type 1 instrument submitted via an Authorized Access ERDS. This is an incident and shall be reported if fraud is suspected.

~~(33) For Type 1 only, unauthorized digital electronic record in a digitized electronic record, or vice versa. This is an incident and shall be reported if fraud is suspected.~~

(314) Unauthorized components that draw data or images from sources external to the digital electronic record or digitized electronic record. This is an incident and shall be reported if intrusion is suspected.

(325) Unauthorized transactions submitted via ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2. This is an incident and shall be reported if fraud is suspected.

(336) For Type 1 only, server failures, including, but not limited to, hardware, software, and network component failures, that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(347) Events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected.

(358) For Type 1 only, unauthorized changes to the ERDS operational configuration. This is an incident and shall be reported if fraud or intrusion is suspected.

(369) For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet. This is an incident and shall be reported if intrusion is suspected.

(3740) For Type 1 only, events for which an ERDS System Administrator is alerted of possible or actual intrusion. This is an incident and shall be reported if intrusion is suspected.

~~(41) For Type 1 only, unauthorized changes to the ERDS operational configuration. This is an incident and shall be reported.~~

(3842) Inability to obtain and employ up-to-date anti-malware software.

(3943) Inability to obtain and employ cryptography, including hashing, encryption and decryption. This is an incident and shall be reported.

~~(44) Use of either compromised or weak encryption algorithms. This is an incident and shall be reported.~~

~~(45) For Type 1 only, discovery of newly published vulnerability existing on a certified ERDS. This is an incident and shall be reported if intrusion is suspected.~~

~~(46) Discovery of susceptibility to newly published exploit. This is an incident and shall be reported if intrusion is suspected.~~

(407) Inability to obtain and employ the most up-to-date patches and hot-fixes.

(418) Unauthorized access or changes to storage media, and improper sanitization of storage media. This is an incident and shall be reported if compromise is suspected.

(429) Any other event that compromises the safety or security of an ERDS. This is an incident and shall be reported.

Note: Authority cited: Section 27393, Government Code. Reference: Sections 27392(b), 27393(b)(2), 27394 and 27396, Government Code.